

EUROPEAN PATENT APPLICATION

Date of publication:

14.03.2001 Patent Gazette 2001/11

Application No.: 00810028.1

Date of application: 12.01.2000

(84) Contracting states cited:

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE

Extension states cited:

AL LT LV MK RO SI

(30) Priority: 07.09.1999 US 152356 P

(71) Applicants: Swisscom AG, 3050 Bern (CH)

(72) Inventors:

- Huber, Adriano

6600 Locarno (CH)

- Loher, Urs, Dr.

3072 Ostermundigen (CH)

(74) Representatives:

Saam, Christophe

Patents & Technology Surveys SA

P.O. Box 1448

2001 Neuchatel (CH)

(54) Method, system and gateway, which allow for an assured end-to-end access to WAP services

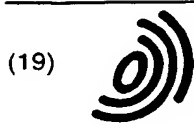
(57) Method by which a mobile subscriber with a WAP-compatible terminal (1) can access to a WAP server or WEB server (5),  
whereby said terminal (1) sends an enquiry for said server to a WAP gateway (3),

whereby the security in the air interface (2) between said WAP-compatible terminal (1) and said gateway (2) is based on WTLS (Wireless Transport Layer Security),

whereby said server (5) is secured with the SSL and/or TLS security protocol,

whereby the conversion between WTLS and SSL and/or TLS takes place in a secured area administered by the administrator of said server (5),

and whereby the packets which are sent from said terminal (1) are forwarded from said gateway (3) to said secured area, without all the packets which are sent during a session being decoded.



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) **EP 1 083 722 A2**

(12) **EUROPÄISCHE PATENTANMELDUNG**

(43) Veröffentlichungstag:  
14.03.2001 Patentblatt 2001/11

(51) Int Cl.7: **H04L 29/06, H04L 12/22,  
H04Q 7/32**

(21) Anmeldenummer: 00810028.1

(22) Anmeldetag: 12.01.2000

(84) Benannte Vertragsstaaten:  
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU  
MC NL PT SE**  
Benannte Erstreckungsstaaten:  
**AL LT LV MK RO SI**

(72) Erfinder:  
• Huber, Adriano  
6600 Locarno (CH)  
• Loher, Urs, Dr.  
3072 Ostermundigen (CH)

(30) Priorität: 07.09.1999 US 152356 P

(74) Vertreter: Saam, Christophe  
Patents & Technology Surveys SA  
P.O. Box 1448  
2001 Neuchâtel (CH)

(71) Anmelder: Swisscom AG  
3050 Bern (CH)

(54) **Verfahren, System und Gateway, die einen End-zu-End gesicherten Zugriff auf WAP-Dienste erlauben**

(57) Verfahren, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät (1) auf einen WAP oder WEB-Server (5) zugreifen kann, wobei das benannte Endgerät (1) eine Anfrage für den benannten Server an ein WAP-Gateway (3) sendet,

wobei die Sicherheit in der Luftschnittstelle (2) zwischen dem benannten WAP-tauglichen Endgerät (1) und dem benannten Gateway (3) auf WTLS (Wireless Transport Layer Security) basiert, wobei der benannte Server (5) mit dem SSL und/

oder TLS Sicherheitsprotokoll gesichert ist, wobei die Konversion zwischen WTLS und SSL und/oder TLS in einem vom Verwalter des benannten Servers (5) verwalteten gesicherten Gebiet erfolgt, und wobei die Pakete, die vom benannten Endgerät (1) gesendet werden, vom benannten Gateway (3) zum benannten gesicherten Gebiet weitergeleitet werden, ohne dass alle Pakete die während einer Session übertragen werden entschlüsselt werden.

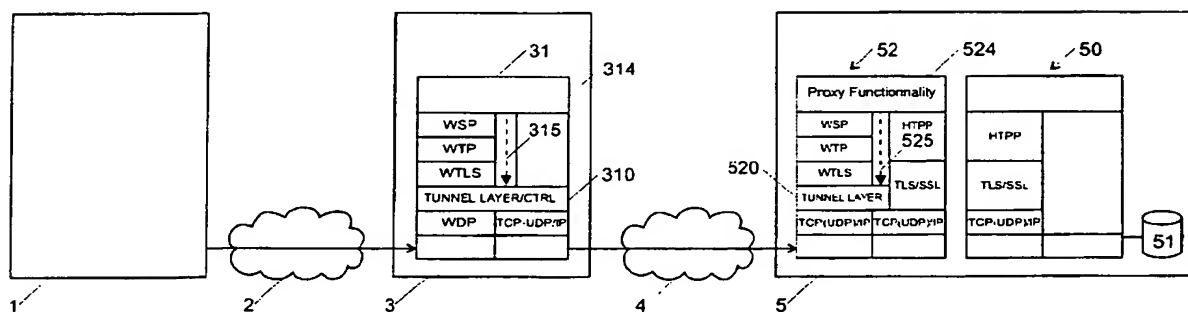


Fig. 3

EP 1 083 722 A2

kann. Die TCP-IP konvertierten Pakete werden an den WAP- oder WEB-Server 50 weitergeleitet, der eventuell eine andere Protokollkonvertierung durchführt, damit die empfangene Abfrage vom Datenbanksystem 51 bearbeitet werden kann.

**[0031]** Als Alternative können die Datagramme mit einem Session-Schlüssel ver- und entschlüsselt werden, dessen Schlüssel mit Hilfe eines zertifizierten, öffentlichen Schlüssel während der Schlüsselvereinbarungsphase generiert werden.

**[0032]** Die Antwort vom WEB bzw. WAP-Server 50, zum Beispiel die gewünschte WEB- oder WAP-Seite, wird vom Server 50 in die andere Richtung gesendet, im Proxy 52 übersetzt und mit WTLS-Diensten gesichert und durch die "Tunnelschicht" 310 im Gateway 31 an das Endgerät 1 des Benutzers geleitet, wobei die gesamte Verbindung zwischen Server 5 und Endbenutzer 1 mit WTLS gesichert wird.

**[0033]** Datagramme, die aufgrund des enthaltenen URL und/oder Portnummer keine End-zu-End gesicherte Datenübertragung verlangen, werden im Gateway 31 gemäss der konventionellen vom WAP-Forum empfohlenen Lösung durch alle Schichten des Protokolls im Gateway 2 entschlüsselt, mit TLS/SSL wieder gesichert und an die in den Paketen angegebene URL-Adresse weitergeleitet. Beispielsweise werden Sessionen mit der Portnummer 80 wie gewöhnliche HTTP-Sessionen behandelt und weitergeleitet.

**[0034]** Antworten vom Server 5 (beispielsweise die gewünschten WEB oder WAP-Seiten) die keine WTLS-Sicherung zwischen Server und Gateway 3 verlangen, werden von der Proxy-Anwendung 524 durch eine Tunnelschicht 520 im Proxy durchgeführt (Pfeil 315) und erst im Gateway 3 mit WTLS-Diensten gesichert.

**[0035]** Diese Variante verlangt keine Änderungen vom Browser im Endgerät 11 und nur ein relativ einfaches Proxy 53 beim Dienstanbieter 5, das WTLS-Sessionen entgegennehmen kann. Die Software-Implementation des Gateways 3 kann sich jedoch als schwierig erweisen.

**[0036]** Die zweite Variante, die auf der Figur 4 dargestellt wird, erlaubt es, dieses Problem durch eine leicht durchführbare Anpassung der Anwendung (zum Beispiel des Browsers) im Endgerät 1 zu vermeiden. In dieser Variante wird die URL-Adresse und die Portnummer der verlangten WEB oder WAP-Seite vom Browser 10 in jedes Paket (WDP-Datagramm) der Session kopiert. Diese Pakete werden dann über das Mobilfunknetz 2 an das Gateway 3 gesendet, wo die Portnummer und die URL analysiert werden, um zu ermitteln wie die Pakete weiterbehandelt werden sollen.

**[0037]** Diese Variante hat den Vorteil, dass die Analyse und die Weiterbehandlung der Pakete in den unteren Schichten des Protokolls, unter anderem in der WDP und/oder WTLS-Schicht, durchgeführt werden kann und dass sie somit nur minimale Anpassungen des Gateways 3 verlangt.

**[0038]** Eine Tabelle 321 im Gateway 3 oder in einem nicht dargestellten Router vor dem Gateway gibt an, wie die Pakete je nach Portnummer und URL behandelt werden sollen und insbesondere welche Pakete transparent durch die Tunnelschicht 320 gehen sollen. Diese Tabelle kann vorzugsweise vom Administrator des Gateways 3 konfiguriert und geändert werden, ohne dass das Gateway neu gestartet werden muss, damit die Konfiguration während des Betriebes aktualisiert werden kann. Daten in der Tabelle können vorzugsweise nur vom Administrator geändert werden, oder von Personen mit Administratorenrechten.

**[0039]** Die Tabelle im Gateway 3 könnte beispielsweise folgende Zeilen enthalten:

	Eingegebene URL Adresse		Neue Adresse (vom Gateway erteilt)		Bemerkung
	Adresse	Portnummer	Adresse	Portnummer	
1	138.10.20.30	8040	140.50.60.70	12345	Pakete mit dieser Adresse werden auf transparente Weise an die neue Adresse geleitet. Die Portnummer wird ersetzt (Mapping).
2	*.*.*.*	50443	*.*.*.*	50443	Stern-Joker erlauben eine Bedingung für alle Server mit der gleichen Portnummer zu setzen
3	138.10.20.40	*	138.10.20.40	*	Wie oben, jedoch ohne DNS-Lookup
4	www.sp1.com	*	www.sp1.com	*	Alle URL vom sp1 müssen durch die Tunnelschicht
5	www.sp1.com	80	www.sp1.com	80	Alle Verbindungen mit Portnummer 80 durch die Tunnelschicht

(fortgesetzt)

	Eingegebene URL Adresse		Neue Adresse (vom Gateway erteilt)		Bemerkung
	Adresse	Portnummer	Adresse	Portnummer	
6	www.sp1.ch	50443	www.sp1.ch	50443	sp1 verlangt, dass alle Sessionen mit der Portnummer 50443 durch die Tunnelschicht geleitet werden.
7	www.sp2.ch	443	www.sp2.ch	443	sp2 verlangt, dass alle Sessionen mit der Portnummer 443 durch die Tunnelschicht geleitet werden. Damit wird kein SSL mit dem Port 443 verwendet. SSL kann dann beispielsweise vom Proxy verwendet werden.
8	...				

**[0040]** Der Administrator des Gateways 3 wird vorzugsweise den Dienst Anbietern einen Bereich von URL-Adressen und/oder Portnummern zur Verfügung stellen. Dienstanbieter SP1, SP2. usw. können dann eine oder mehrere URL, oder Portnummern, oder Kombinationen aus beiden, für sich reservieren und den Administrator 3 anweisen, Pakete mit dieser URL und/oder Portnummer transparent weiterzuleiten.

**[0041]** Die Figur 5 zeigt als Beispiel, wie die Pakete, die von verschiedenen Endbenutzern  $1_1$  bis  $1_4$  gesendet werden, vom Gateway 3 in Abhängigkeit ihrer URL-Adresse und/oder Portnummer behandelt werden.

**[0042]** Das dargestellte System umfasst in diesem Beispiel drei Server  $5_1$ ,  $5_2$  und  $5_3$  von drei verschiedenen Dienst Anbietern sp1, sp2 und sp3. Die vier folgenden Seiten werden im ersten Server  $5_1$  (bzw.  $5_2$ ) abgelegt:

- eine ungesicherte WEB-Seite mit der Adresse www.sp1.com:80 (bzw. www.sp2.com:80)
- eine WEB-Seite mit der Adresse www.sp1.com:443 (bzw. www.sp2.com:443), die nur mit SSL gesichert wird (keine End-zu-End Sicherheit)
- eine WEB-Seite mit der Adresse www.sp1.com:50443 (bzw. www.sp2.com:50443), die mit WTLS gesichert wird (End-zu-End Sicherheit)
- eine WAP-Seite mit der Adresse wap.sp1.com:50443 (bzw. wap.sp2.com:50443), die mit WTLS gesichert wird (End-zu-End Sicherheit)

**[0043]** Im Server  $5_3$  des dritten Dienst Anbieters sp3 werden nur zwei Seiten abgelegt:

- eine ungesicherte WEB-Seite mit der Adresse www.sp3.com:80
- eine WEB-Seite mit der Adresse www.sp3.com:443, die nur mit SSL gesichert wird (keine End-zu-End Sicherheit)

**[0044]** Der erste Benutzer  $1_1$  will auf die gesicherten Seiten www.sp1.com:443 und www.sp1.com:50443 des Dienst-anbieters SP1 im Server  $5_1$  zugreifen, indem er GET(URL) Abfragen mit entsprechenden URL an das Gateway 3 sendet. Das Gateway 3 erkennt anhand der Tabelle 321 und des im Datagramm enthaltenen URL und/oder der Portnummer, welche Sicherheiten von diesen Seiten verlangt werden. Im ersten Fall (SSL Sicherheit) werden alle Datagramme der Session im Gateway 3 entschlüsselt und eine Übersetzung von WTLS zu SSL wird durchgeführt. Im zweiten Fall (End-zu-End Sicherheit mit WTLS) werden alle Datagramme der Session transparent an den Server  $5_1$  weitergeleitet, ohne dass sie entschlüsselt werden.

**[0045]** Der zweite Benutzer  $1_2$  will auf die Seite www.sp2.com:50443 des Dienst-anbieters sp2 im Server  $5_2$  zugreifen, die eine End-zu-End Sicherheit verlangt. Datagramme mit dieser Adresse werden im Gateway 3 erkannt und transparent durch die Tunnelschicht an den Server  $5_2$  geleitet.

**[0046]** Der dritte Benutzer  $1_3$  will auf die Seite www.sp3.com:443 des Dienst-anbieters sp2 im Server  $5_2$  zugreifen, die eine mit TLS/SSL gewährleistete Sicherheit verlangt. WTLS-gesicherte Datagramme mit dieser Adresse werden im Gateway 3 erkannt, durch alle Schichten des Protokoll-Stapels übersetzt, mit TLS/SSL gesichert und an den Server  $5_3$  weitergeleitet.

[0047] Der vierte Benutzer 1<sub>4</sub> will auf die ungesicherte Seite www.sp3.com:80 des Dienstbieters sp2 im Server 5<sub>2</sub> zugreifen. WTLS-gesicherte Pakete mit dieser Adresse werden im Gateway 3 erkannt, durch alle Schichten des Protokoll-Stapels übersetzt und an den Server 5<sub>3</sub> weitergeleitet, ohne sie durch das Netz 4 zu sichern.

[0048] Diese Variante verlangt nur minimale Änderungen vom Gateway 3. Allerdings müssen die Browser-Anwendungen in den Endgeräten 1 leicht angepasst werden, was sich bei vielen Anbietern als schwierig erweisen kann.

[0049] Wir werden jetzt eine dritte Erfindungsvariante beschreiben, die diesen Nachteil vermeidet.

[0050] In dieser Variante werden Sessionen die eine End-zu-End Sicherheit verlangen anhand der URL-Adresse und/oder der Portnummer wie in der ersten oder zweiten Variante erkannt. Statt die Sessionen durch die Tunnelschicht transparent weiterzuleiten, sendet das Gateway in diesem Fall einen standardisierten Redirect-Befehl mit der in der Tabelle 321 angegebenen Adresse und Portnummer des Dienstbieters und mit anderen Parameter für die Identifizierung vom Gateway 5, wie Dial-In Nummer, an das Endgerät 1.

[0051] Die Weiterleitungsadresse (Adresse, Portnummer, Dial-In Nummer, usw.) im Redirect-Befehl wird vorzugsweise aus einem vom WAP oder WEB-Server 5 zugänglich gemachten Dokument extrahiert. Der Redirect-Befehl kann auch dieses oder ein anderes Dokument oder die Adresse eines solchen Dokuments enthalten, in welchem die Weiterleitungsadresse enthalten ist. Im Dokument können vorzugsweise verschiedene Adressengebiete mit Stringmuster, beispielsweise mit \*, angegeben werden.

[0052] Die Anwendung im Mobilgerät 1, die diesen Redirect Befehl entgegennimmt, reagiert, indem sie jetzt die schon vorher an das Gateway 3 gesendeten Pakete wieder direkt an die im Redirect-Befehl angegebene Adresse des Dienstbieters sendet.

[0053] Alle Pakete in der Session werden dann direkt zwischen dem Endgerät 1 und dem Server 5 übertragen, bis der Endbenutzer einen anderen URL sendet, der vom Server 5 nicht bearbeitet werden kann (beispielsweise wenn sich die entsprechende gewünschte Seite nicht auf diesem Server befindet). In diesem Fall wird die Session vom Server 5 unterbrochen und die nachfolgenden Pakete werden wieder an das Gateway 3 gesendet.

[0054] Falls keine End-zu-End Sicherheit benötigt wird, wird kein Redirect Befehl vom Gateway 3 gesendet. In diesem Fall werden alle Pakete während der gesicherten Session durch das Gateway 3 gesendet.

#### Patentansprüche

1. Verfahren, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät (1) auf einen WAP oder WEB-Server (5) zugreifen kann, wobei das benannte Endgerät (1) eine Anfrage für den benannten Server an ein WAP-Gateway (3) sendet,

wobei die Sicherheit in der Luftschnittstelle (2) zwischen dem benannten WAP-tauglichen Endgerät (1) und dem benannten Gateway (3) auf WTLS (Wireless Transport Layer Security) basiert, wobei der benannte Server (5) mit dem SSL und/oder TLS Sicherheitsprotokoll gesichert ist,

dadurch gekennzeichnet, dass die Konversion zwischen WTLS und SSL und/oder TLS in einem vom Verwalter des benannten Servers (5) verwalteten gesicherten Gebiet erfolgt,

und dass die Pakete, die vom benannten Endgerät (1) gesendet werden, vom benannten Gateway (3) zum benannten gesicherten Gebiet weitergeleitet werden, ohne alle Pakete die während einer Session übertragen werden zu entschlüsseln.

2. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass das benannte Gateway (3) die benannten Pakete zu einem Proxy (52) im benannten gesicherten Gebiet weiterleitet, wobei das benannte Proxy (52) mindestens eine Protokollschicht des WAP-Protokolls verwendet.

3. Verfahren gemäss einem der Ansprüche 1 oder 2, in welchem die benannten Pakete in Abhängigkeit vom URI und/oder vom Domainname der angefragte Seite im benannten Gateway (3) weitergeleitet werden.

4. Verfahren gemäss einem der vorhergehenden Ansprüche, in welchem die benannten Pakete abhängig von der Portnummer im benannten Gateway (3) weitergeleitet werden.

5. Verfahren gemäss dem vorhergehenden Anspruch, in welchem die benannten Pakete abhängig von verschiedenen Portnummern an verschiedene gesicherte Gebiete weitergeleitet werden.

6. Verfahren gemäss einem der Ansprüche 4 oder 5, in welchem die benannte Portnummer aus der URI und/oder URL der angefragten Seite in einer Anwendungsschicht des benannten Gateways (3) extrahiert werden.

7. Verfahren gemäss Anspruch 6, in welchem die benannte Portnummer während einer Session nur aus einer begrenzten Anzahl von Paketen extrahiert wird,  
und in welchem das Weiterleiten von mindestens einem folgenden Paket von dieser benannten extrahierten Portnummer abhängig ist.
8. Verfahren gemäss Anspruch 7, in welchem ein Proxyserver (52) im benannten gesicherten Gebiet die URI und/oder die Portnummer der empfangenen Pakete extrahiert, und in welchem der benannte Proxyserver (52) dem benannten Gateway (3) einen Befehl zurücksendet, wenn er ein Paket mit einer anderen URI und/oder mit einer anderen Portnummer empfängt.
9. Verfahren gemäss einem der Ansprüche 4 oder 5, in welchem die benannte Portnummer aus dem benannten URI und/oder URL der angefragten Webseite im benannten Endgerät (1) extrahiert wird.
10. Verfahren gemäss Anspruch 9, in welchem die benannte Portnummer von einem Browser aus dem URI und/oder URL der angefragten Webseite extrahiert wird.
11. Verfahren gemäss einem der Ansprüche 8 oder 9, in welchem der Browser im benannten Endgerät (1) die benannte Portnummer in den benannten Paketen erst dann kopiert, wenn eine End-zu-End gesicherte Verbindung beantragt ist.
12. Verfahren gemäss einem der Ansprüche 3 bis 11, in welchem die benannten Pakete im benannten Gateway (3) an ein gesichertes Gebiet weitergeleitet werden wenn sich die benannte Portnummer in einem vorbestimmten Bereich befindet.
13. Verfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass wenn eine End-zu-End gesicherte Verbindung beantragt ist, das benannte Gateway (3) einen Redirect-Befehl zum benannten Endgerät (1) sendet.
14. Verfahren gemäss dem vorhergehenden Anspruch, in welchem der benannte Redirect Befehl zeitlich begrenzt ist.
15. Verfahren gemäss Anspruch 13, in welchem ein Proxy Server (52) im benannten gesicherten Gebiet die URI und/oder die Portnummer der empfangenen Pakete extrahiert, und einen Redirect Befehl zurück zum benannten Endgerät (1) sendet, sobald die Session zum benannten Gateway (3) weitergeleitet werden soll.
16. Verfahren gemäss Anspruch 13, in welchem den benannten Redirect-Befehl eine Weiterleitungsadresse enthält, die aus einem vom benannten WAP oder WEB-Server (5) zugänglich gemachten Dokument extrahiert wird.
17. Verfahren gemäss dem Anspruch 13, in welchem den benannten Redirect-Befehl ein Dokument enthält, in welchem die Weiterleitungsadresse enthalten ist.
18. Verfahren, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät (1) auf einen WAP oder WEB-Server (5) zugreifen kann,  
wobei das benannte Endgerät (1) eine Anfrage für den benannten Server (5) an ein WAP-Gateway (3) sendet, dadurch gekennzeichnet, dass ein Browser im benannten Endgerät (1) die Portnummer der beantragten WEB oder WAP-Seite extrahiert und in zum benannten Gateway (3) gesendete Paketen kopiert,  
und dass die benannten Pakete im benannten Gateway (3) in Abhängigkeit von dieser Portnummer weitergeleitet werden.
19. Gateway (3), das mit WTLS-gesicherte Datagramme von WAP-tauglichen Endgeräten entgegennehmen und in SSL-gesicherte-Abfragen übersetzen kann,  
dadurch gekennzeichnet, dass es Datagramme erkennen kann, die in transparenter Weise weitergeleitet werden sollen und dass es diese Datagramme ohne sie zu entschlüsseln weiterleiten kann.
20. Gateway gemäss dem vorhergehenden Anspruch, in welchem die benannten Pakete in Abhängigkeit vom URI und/oder vom Domainname der angefragten Seite weitergeleitet werden.
21. Gateway gemäss einem der Ansprüche 19 oder 20, in welchem die benannten Pakete in Abhängigkeit von der Portnummer im benannten Gateway (3) weitergeleitet werden.

## EP 1 083 722 A2

22. Gateway gemäss dem vorhergehenden Anspruch, in welchem die benannten Pakete abhängig von verschiedenen Portnummern an verschiedene gesicherte Gebiete weitergeleitet werden.
- 5 23. Gateway gemäss einem der Ansprüche 21 oder 22, in welchem die benannte Portnummer aus dem URI und/oder URL der angefragten Seite in einer Anwendungsschicht des benannten Gateways (3) extrahiert werden.
24. Gateway gemäss Anspruch 21, in welchem die benannte Portnummer während einer Session nur aus einer begrenzten Anzahl von Paketen extrahiert werden,  
10 und in welchem das Weiterleiten von mindestens einem folgenden Paket von dieser benannten extrahierten Portnummer abhängig ist.

15

20

25

30

35

40

45

50

55

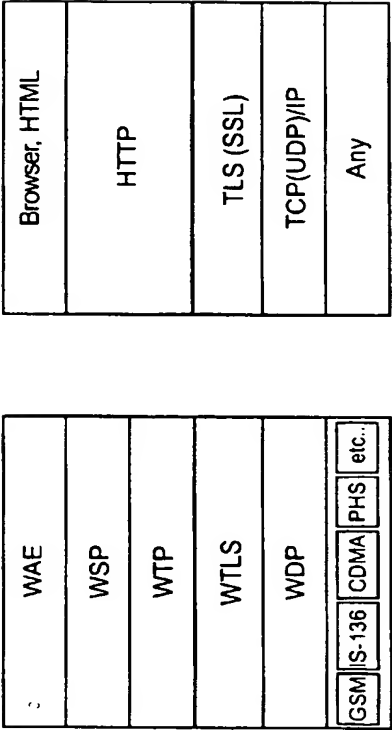


Fig. 1



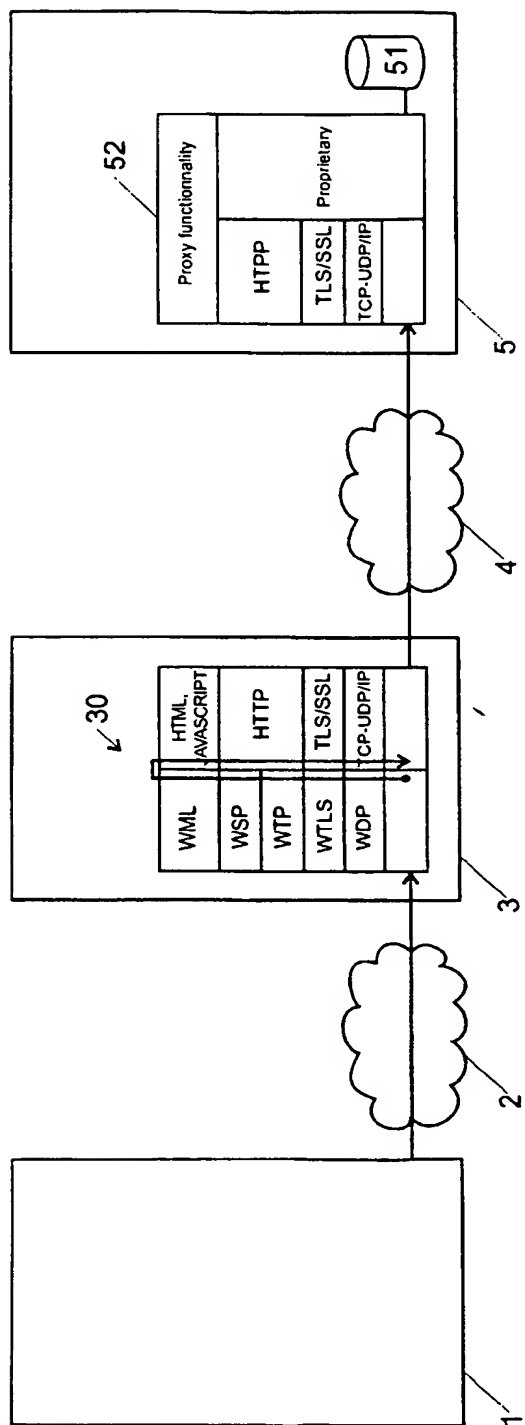


Fig. 2

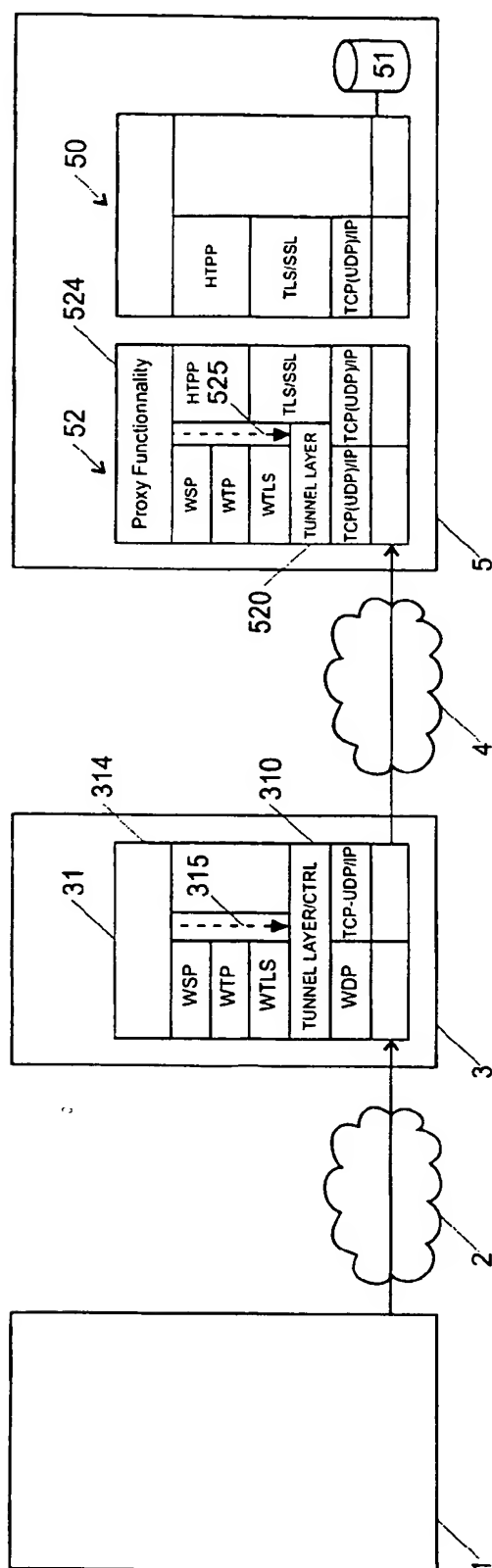


Fig. 3

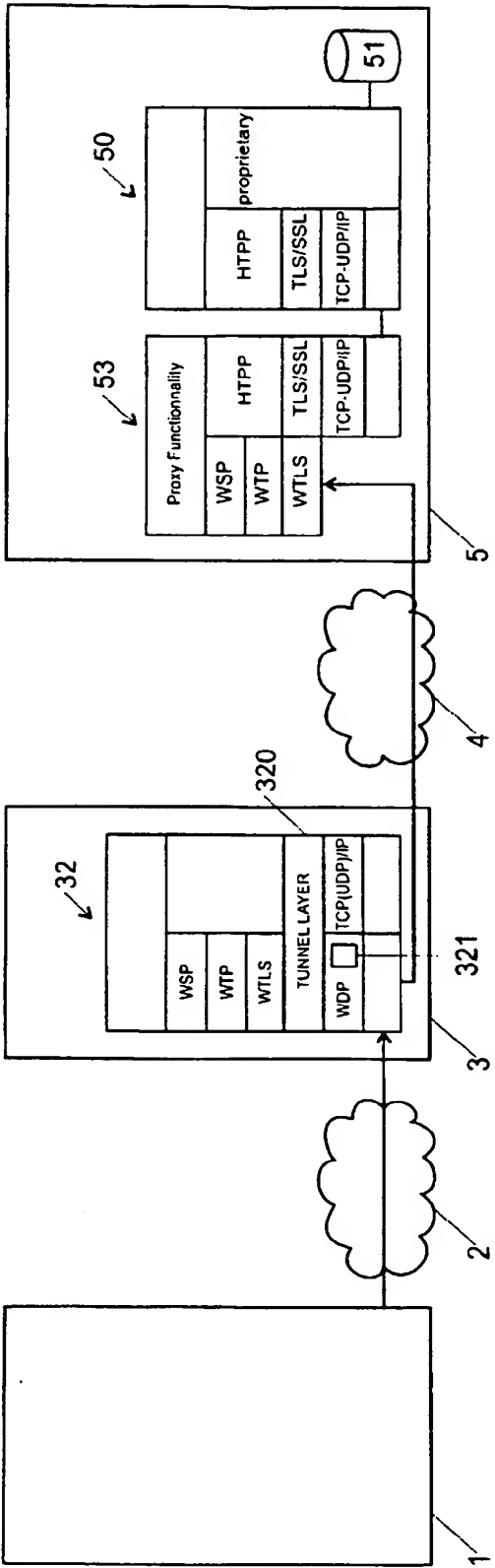


Fig. 4

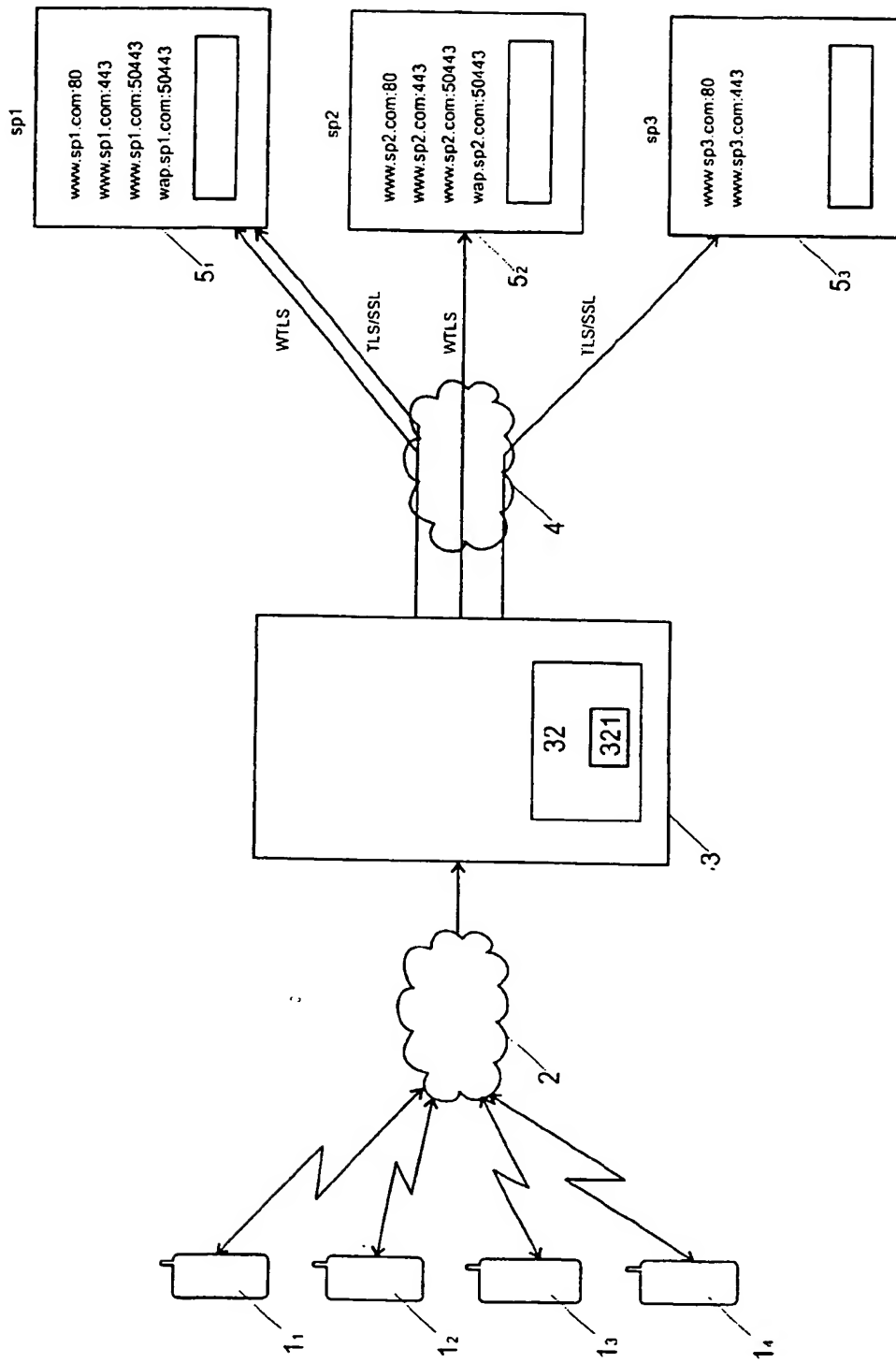
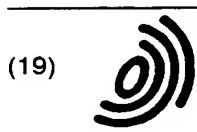


Fig. 5



Europäisches Patentamt  
European Patent Office  
Office européen des brevets



(11) **EP 1 083 722 A3**

(12)

## EUROPÄISCHE PATENTANMELDUNG

(88) Veröffentlichungstag A3:  
18.07.2001 Patentblatt 2001/29

(51) Int Cl.7: **H04L 29/06**, **H04L 12/22**,  
**H04Q 7/32**, **H04L 29/08**,  
**H04L 12/56**

(43) Veröffentlichungstag A2:  
14.03.2001 Patentblatt 2001/11

(21) Anmeldenummer: **00810028.1**

(22) Anmeldetag: **12.01.2000**

(84) Benannte Vertragsstaaten:  
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU**  
**MC NL PT SE**  
Benannte Erstreckungsstaaten:  
**AL LT LV MK RO SI**

(72) Erfinder:  
• **Huber, Adriano**  
**6600 Locarno (CH)**  
• **Loher, Urs, Dr.**  
**3072 Ostermundigen (CH)**

(30) Priorität: **07.09.1999 US 152356 P**

(74) Vertreter: **Saam, Christophe et al**  
**Patents & Technology Surveys SA**  
**P.O. Box 1448**  
**2001 Neuchâtel (CH)**

(71) Anmelder: **Swisscom Mobile AG**  
**3050 Bern (CH)**

(54) **Verfahren, System und Gateway, die einen End-zu-End gesicherten Zugriff auf WAP-Dienste erlauben**

(57) Verfahren, mit welchem ein Mobilteilnehmer mit einem WAP-tauglichen Endgerät (1) auf einen WAP oder WEB-Server (5) zugreifen kann, wobei das benannte Endgerät (1) eine Anfrage für den benannten Server an ein WAP-Gateway (3) sendet,

wobei die Sicherheit in der Luftschnittstelle (2) zwischen dem benannten WAP-tauglichen Endgerät (1) und dem benannten Gateway (2) auf WTLS (Wireless Transport Layer Security) basiert, wobei der benannte Server (5) mit dem SSL und/

oder TLS Sicherheitsprotokoll gesichert ist, wobei die Konversion zwischen WTLS und SSL und/oder TLS in einem vom Verwalter des benannten Servers (5) verwalteten gesicherten Gebiet erfolgt,

und wobei die Pakete, die vom benannten Endgerät (1) gesendet werden, vom benannten Gateway (3) zum benannten gesicherten Gebiet weitergeleitet werden, ohne dass alle Pakete die während einer Session übertragen werden entschlüsselt werden.

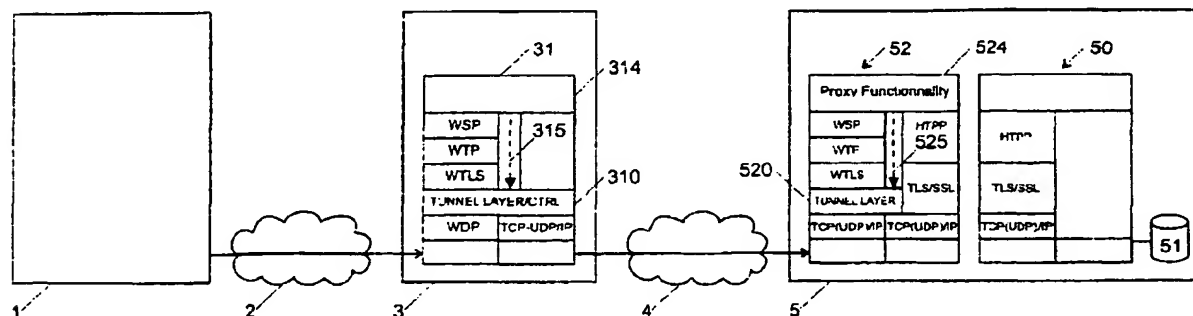


Fig. 3



Europäisches  
Patentamt

EUROPÄISCHER RECHERCHENBERICHT

Nummer der Anmeldung  
EP 00 81 0028

EINSCHLÄGIGE DOKUMENTE			
Kategorie	Kennzeichnung des Dokuments mit Angabe, soweit erforderlich, der maßgeblichen Teile	Betrifft Anspruch	KLASSIFIKATION DER ANMELDUNG (Int.Cl.7)
P,A	WO 99 45684 A (NOKIA MOBILE PHONES LTD ;NYKAENEN PETRI (FI)) 10. September 1999 (1999-09-10) * Seite 11, Zeile 7 - Seite 13, Zeile 19 * * Seite 15, Zeile 16-19 *	1,18,19	H04L29/06 H04L12/22 H04Q7/32 H04L29/08 H04L12/56
A	& FI 980 485 A (NOKIA MOBILE PHONES LTD) 4. September 1999 (1999-09-04) * das ganze Dokument *	1,18,19	
A	LUOTONEN A: "Tunneling SSL Through a WWW Proxy" INTERNET DRAFT, 14. Dezember 1995 (1995-12-14), XP002167506 Internet Engineering Task Force (IETF) * das ganze Dokument *	1,18,19	
P,A	JORMALAINEN S AND LAINE J: "Security in the WTLS" SEMINAR ON NETWORK SECURITY, 'Online! 3. - 30. November 1999, XP002167503 Helsinki Gefunden im Internet: <URL:http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/wtls/wtls.html> 'gefunden am 2001-05-16! * Absatz '03.2!' *	1,18,19	
P,O, A	-& HELSINKI UNIVERSITY OF TECHNOLOGY: "Seminar Program" SEMINAR ON NETWORK SECURITY, 'Online! 2. - 3. November 1999, Seite 03-11- XP002167504 Helsinki Gefunden im Internet: <URL:http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/seminar.html> 'gefunden am 2001-05-16! * Absätze '0III!-'0002!' *	1,18,19	
Der vorliegende Recherchenbericht wurde für alle Patentansprüche erstellt			RECHERCHIERTE SACHGEBIETE (Int.Cl.7) H04L
Recherchenort DEN HAAG		Abschlußdatum der Recherche 23. Mai 2001	Prüfer Dupuis, H
KATEGORIE DER GENANNTEN DOKUMENT		T : der Erfindung zugrunde liegende Theorien oder Grundsätze E : älteres Patentedokument, das jedoch erst am oder nach dem Anmeldedatum veröffentlicht wurden ist D : in der Anmeldung angeführtes Dokument L : aus anderen Gründen angeführtes Dokument & : Mitglied der gleichen Patentfamilie, übereinstimmendes Dokument X : von besonderer Bedeutung allein betrachtet Y : von besonderer Bedeutung in Verbindung mit einer anderen Veröffentlichung derselben Kategorie A : technologischer Hintergrund O : nichtschriftliche Offenbarung P : Zwischenliteratur	

EP 1 083 722 A3 (1999-09-10)

